AliExpress -60% ГЛАВНАЯ РАСПРОДАЖА ГОДА 11.11 AliExpress
11.11 на AliExpress.
Всемирный день шопинга.
AliExpress Открыть

Blog der belarussischen Bärin (ex_petra_le) написал в minsk_by
2007-04-16 19:30:00

Категория: IT

Сайты Третьего Пути и партнеров уничтожены хакерской атакой

Вечером 16 апреля проявив «солидарность» с волной наездов на «Третий Путь» из оппозиционной среды хакеры называющиеся себя Anti oppozition forces найдя брешь в защите стерли на сервере Третьего Пути следующие сайты сообщества: www.3dway.org, www.belzhaba.com, www.multclub.org и др., а также сайты наших партнеров: Офиса «За демократическую Беларусь»: www.democraticbelarus.eu, Беларусы.ЕУ: www.belarusy.eu, Андрея Суздальцева: www.politoboz.com.

Видимо выйдя на работу в Понедельник наши «коллеги» в органах госбезопасности озаботились судьбой господина Волчека и чистотой мундира полковника Подобеда и решили их морально поддержать.
Подписались "херои" как
Hack3d by AntiOppositionForce {AntiPartizan}

Мы не будем восстанавливать сайты сразу в полном объеме, а не спеша проанализируем их защиту и будем включать их по очереди, убедившись в том, что они защищены.

Приносим извинения нашим партнерам и нашим читателям за временные неудобства.

Техническая служба «Третьего Пути»

Подписаться

Надоела реклама? Улучшите аккаунт всего за $1.66 в месяц!

ДОБАВИТЬ КОММЕНТАРИЙ — 77 комментариев

< 1 2 >

altavetra
16 апреля 2007, 21:37:32 UTC

ВОССТАНАВЛИВАЙТЕСЬ!

ОТВЕТИТЬ НРАВИТСЯ

chris_gomel
16 апреля 2007, 22:04:39 UTC

Мда, а два вялікіх файлы перамоваў на Плошчы я так і не паспела спампаваць...
Мдя.

ОТВЕТИТЬ НРАВИТСЯ

ex_petra_le
16 апреля 2007, 22:21:14 UTC

Усё будзе добра!
а пакуль што можаце глянуць і падняць настрой ;)
http://www.belzhaba.com/
http://www.3dway.org/

ОТВЕТИТЬ НРАВИТСЯ

verasen
17 апреля 2007, 15:19:46 UTC

давай на пошту табе залью)

ОТВЕТИТЬ НРАВИТСЯ

polyethylenimin
17 апреля 2007, 00:19:48 UTC

похоже вам шимбздец. Минимум замена хостинга и мастер-класс для админа. Хоть вас и не люблю, но больше сайтов хороших и разных должно быть.

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

algizzz
17 апреля 2007, 00:24:10 UTC

О, привет! Да я думаю, это все фикция.

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

polyethylenimin
17 апреля 2007, 00:30:52 UTC

думаю нет, такие "серверы" ломаются на раз. Хотя малчеги неприятные сами по себе.

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

devnu11
17 апреля 2007, 04:55:20 UTC

Делай раз

%host 3dway.org
3dway.org has address 81.222.134.156
3dway.org mail is handled by 20 mx2.spaceweb.ru.
3dway.org mail is handled by 10 mx1.spaceweb.ru.
%

Делай два

http://81.222.134.156

Делай три

новости
[2007-04-16]
Доменная революция!
.....
Также производится ежесуточное резервное копирование всей информации наших клиентов (backup).

Вы еще кипятите ? А мы уже рубим. И скоро придем к Вам! Революцию в массы! ;)
Да уж. Ничего хорошего не скажешь о сайтах, размещенных на shared аккаунтах. Много проблем отсюда растет. Теоретически, взломав любой сайт, расположенный на shared сервере, можно облегчить себе задачу для поиска бреши в защите конечного сайта с того же сервера.Да, еще в догонку - http://www.domaintools.com/rbl/?ip=81.222.134.156. Да не суть важно. Спам не их. Они просто разместили сайт.

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

macsim_by
17 апреля 2007, 09:31:57 UTC

т.е. ТП в России хостился? ;)

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

devnu11
17 апреля 2007, 12:51:30 UTC

таки да :)
фрагмент traceroute:

19 77 ms 77 ms 77 ms 81.222.223.10
20 79 ms 79 ms 78 ms 81.9.3.66
21 78 ms 77 ms 77 ms 81.222.134.156

Предпоследний хоп, исходя из http://www.dnsstuff.com/tools/ipall.ch?ip=81.9.3.66. находится в

IP address: 81.9.3.66.
Country (per IP registrar): RU [Russian Federation]
City (per outside source): St. Petersburg, Sankt-Peterburg

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

macsim_by
17 апреля 2007, 17:58:31 UTC

крута! ;) молодцы! они бы ещё в РБ швейцарский хостинг купили ;)

а ведь когда-то они говорили, что их защита выдерживала атаки, когда другие сайты валились, ТП стоял, как хм... штык! ;)

ОТВЕТИТЬ РАЗВЕРНУТЬ НРАВИТСЯ

eternal_leave 13 лет назад РАЗВЕРНУТЬ
macsim_by 13 лет назад РАЗВЕРНУТЬ
devnu11 13 лет назад РАЗВЕРНУТЬ
macsim_by 13 лет назад РАЗВЕРНУТЬ

algizzz
17 апреля 2007, 00:23:13 UTC

Лучше проанализируйте логи, если они есть, конечно, и выложите результаты.

ОТВЕТИТЬ НРАВИТСЯ

macsim_by
17 апреля 2007, 09:33:31 UTC

оба-на, Звёздные войны! "Империя наносит ответный удар"! ;) Ждём серию "Возвращение джедая"! ;)

ОТВЕТИТЬ НРАВИТСЯ

macsim_by
17 апреля 2007, 09:38:34 UTC

whois 81.222.134.156

% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
% To receive output for a database update, use the "-B" flag

% Information related to '81.222.134.0 - 81.222.135.255'

inetnum: 81.222.134.0 - 81.222.135.255
netname: SpaceWeb
descr: PROVIDER
country: RU
admin-c: KAPY-RIPE
tech-c: KAPY-RIPE
status: ASSIGNED PA
mnt-by: ELTEL-RIPE-MNT
source: RIPE # Filtered

person: Nikita V Kapitansky
address: 53A, 2-nd Line,
address: Vasilievsky Island
address: St-Petersburg, 199004, Russia
e-mail: manager@sweb.ru
phone: +7 812 3271923
fax-no: +7 812 3271923
nic-hdl: KAPY-RIPE
source: RIPE # Filtered

% Information related to '81.222.128.0/20AS20597'

route: 81.222.128.0/20
descr: ELTEL.net
origin: AS20597
mnt-by: ELTEL-RIPE-MNT
source: RIPE # Filtered

ОТВЕТИТЬ НРАВИТСЯ

:)
antipartizan
17 апреля 2007, 17:01:16 UTC

http://antipartizan.livejournal.com/

ОТВЕТИТЬ НРАВИТСЯ

ДОБАВИТЬ КОММЕНТАРИЙ — 77 комментариев

< 1 2 >

Покупайте технику по выгодным ценам. ОТКРЫТЬ
Надоела реклама? Улучшите аккаунт всего за $1.66 в месяц!